

УДК 004.056

Паньків Т. – ст. гр. СН – 41

Тернопільський національний технічний університет імені Івана Пулюя

ПРОБЛЕМА БЕЗПЕКИ СУЧАСНИХ CMS

Науковий керівник: к.т.н., доцент Мацюк О.В.

Сучасні вимоги до веб-вузлів зобов'язують використовувати новий підхід до розробки. Інформація, яка розміщується на веб-вузлах, повинна швидко оновлюватися. Для вирішення цього завдання створюються системи керування вмістом (CMS), які дозволяють легко змінювати наповнення сайту через інтуїтивно зрозумілий інтерфейс. "Система управління контентом", або CMS - останнім часом один з найпоширеніших способів адміністрування веб-порталу. Все більше число студій веб-дизайну пропонують створення сайтів на різних CMS.

Всі існуючі CMS не гарантують безпеку веб-сервера навіть для масштабів середнього бізнесу. Кожна компанія має проблеми з безпекою корпоративного сайту, і перш за все ці проблеми пов'язані з уразливістю системи управління вмістом. Для підтримки системи управління потрібний системний адміністратор, що значно збільшує витрати на експлуатацію та не гарантує повної безпеки. Величезне значення має людський фактор.

Для розробки концепції захищеної системи управління необхідно також розглянути переваги та недоліки більшості систем управління.

Основна перевага CMS - це зручність редагування і додавання на сайт нового вмісту. Крім того, системи управління сайтом дозволяють швидко і зручно редагувати сторінки новин, гостьові книги, форуми, блоги та багато іншого. Дуже зручний у використанні візуальний редактор, що зустрічається у багатьох CMS.

Недоліком більшості CMS є динамічна адресація. Приклад: стандартна адресація в CMS Joomla дозволяє атакуючому легко змінювати значення переданих змінних, що ставить під загрозу всю систему безпеки. Також використання динамічної адресації є небажаним для реєстрації сайту пошуковими системами. Майже у всіх CMS для вирішення цієї проблеми використовується функція `mod_rewrite`, проте не завжди підтримується компаніями, що надають послуги хостингу. У результаті роботи `mod_rewrite` відбувається підміна адреси запиту, на адресу, що не містить імен змінних. Проте використання функції `mod_rewrite` не дозволяє захистити CMS від передачі видозмінених змінних. У цьому випадку вся обробка та виявлення атак лягає на систему управління. Це допускає можливість використання досить широкого спектру атак, що таким способом реалізують SQL-injection.

Будь-яка система управління містить вразливості, це може служити причиною взлому сайту і сервера. Оновлення системи управління є досить складною процедурою. Більшість систем управління не дозволяють здійснити оновлення повністю автоматично, тому цим займаються адміністратори. Цю проблему можна вирішити тільки за допомогою системи активних оновлень. Тобто оновлення здійснюється автоматично. У більшості систем керування автоматичні оновлення здійснюються частково за запитом адміністратора з системи управління.

Більшість CMS здійснюють неповний аналіз переданих параметрів. Саме на цьому рівні можна захистити систему управління від атак SQL-injection і PHP-including.